Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ	**УТВЕРЖДАЮ**
Декан, председатель совета Факультета КТВТиЭ.	Проректор по учебной работе, председатель методического совета ДГТУ
_____ Ш.А. Юсуфов	_____ Н. С. Суракатов
Подпись ИОФ	Подпись ИОФ
20 09 2018г.	24 09 2018г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Б1.В.ОД.8 – «Прикладная алгебра»
наименование дисциплины по ООП и код по ФГОС
для направления 01.03.02 – Прикладная математика и информатика
по профилю – «Системное программирование и компьютерные технологии»
шифр и полное наименование направления (специальности)
факультет Компьютерных технологий, вычислительной техники и энергетики
наименование факультета, где ведется дисциплина
кафедра Высшей математики
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) бакалавр
бакалавр (специалист)

Форма обучения очная, курс 3,4 семестр (ы) 6, 7
очная, заочная, др.
Всего трудоемкость в зачетных единицах (часах) 7 ЗЕТ (252 часа) :
лекции 51 (час.); экзамен 7 (13ЕТ – 36 час) ;
(семестр)
практические (семинарские) занятия - (час); зачет 6
(семестр)
лабораторные занятия 68 ; самостоятельная работа 97 (ч.);
курсовой проект (работа, РГР) - (семестр).

Зав. кафедрой _____ А.М. Нурмагомедов
подпись ИОФ

Начальник УО _____ Э.В. Магомаева
подпись ИОФ

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ООП ВО для направления 01.03.02 – Прикладная математика и информатика, по профилю – «Системное программирование и компьютерные технологии».

Программа одобрена на заседании выпускающей кафедры

от 16.09 года, протокол № 1.

Зав. выпускающей кафедрой по данному направлению (специальности, профилю)

_____ Т.И. Исабекова
подпись ИОФ

ОДОБРЕНО:

Методической комиссией по укрупненной группе специальностей и направлений 01.00.00 – Математика и механика

Председатель МК:

_____ Т.И. Исабекова
подпись ИОФ

«16» 09 2014.

АВТОР ПРОГРАММЫ:

к.ф.-м.н., ст. преп. каф. ВМ
уч. степень, ученое звание

_____ Р.А. Ханров
подпись *ИОФ*

1. Наименование и общее описание дисциплины

Дисциплина "Прикладная алгебра" обеспечивает подготовку по одной из фундаментальных математических дисциплин, являющейся важным инструментом исследования многих задач естествознания и техники.

2. Место дисциплины в структуре ООП.

Целями освоения дисциплины являются изучение основных понятий и методов современной прикладной алгебры и умение применять их при решении практических задач. Одной из основных целей курса является знакомство студентов с основными конструкциями абстрактной алгебры, элементарной теории чисел и теории решеток, используемых в прикладных исследованиях.

Требования к результатам освоения дисциплины:

Раздел 1.Основные алгебраические структуры: группы, кольца, поля.

Раздел 2.Центральная роль отведена конечным полям, приводится классический пример их приложений – построение кодов, исправляющих ошибки.

Раздел 3.Методы решений прикладных задач кодирования.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины.

Выпускник должен обладать следующими общепрофессиональными компетенциями (ОПК):

- способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с прикладной математикой и информатикой (ОПК-1);
- способностью к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям (ОПК-3);
- способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4).

профессиональными компетенциями (ПК):

- способностью собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям (ПК-1);

способностью понимать, совершенствовать и применять современный математический аппарат (ПК-2);

- способностью формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций (ПК-6);

В результате изучения дисциплины студент должен:

знать: представление об основных алгебраических структурах, используемых в перечислительных и алгоритмических задачах, в том числе о конечных группах и полях Галуа

уметь: пользоваться методами абстрактной алгебры для формализации и решения прикладных задач, в том числе в некоторых задач криптографии и теории кодирования;

владеть: математическими основами современной прикладной теории решеток, используемой в ряде методов представления и анализа информации.

4. Объём дисциплины

Объём дисциплины Б1.В.ОД.8 – «Прикладная алгебра» составляет 7 ЗЕТ (252 часа). Из них на аудиторные занятия отведены 119 часов (лекции 51 час, лабораторные занятия – 68 часов), на самостоятельную работу 97 часов.

4. Структура и содержание дисциплины

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины. Тема лекции и вопросы	Семестр	Неделя семестра	Виды учебной работы, включая СР студентов и трудоемкость в часах			Формы текущего контроля успеваемости (по срокам аттестации) в семестре. Форма промежуточной аттестации по семестрам
				лк	пз	ср	
1.	**Лекция 1. Группы.** Введение. Алгебра. Алгебраические операции. Группа (определение, простейшие свойства, примеры, терминология). Все конечные группы малых порядков. Симметрические группы. Циклические группы. Подгруппы. Все конечные группы малых порядков. Симметрические группы. Циклические группы. Подгруппы.	6	1, 2	2	4	5	Входная контрольная работа
2.	**Лекция 2.** Группа автоморфизмов. Перестановки. Теорема Кэли. Смежные классы. Отношение эквивалентности в группе (через принадлежность смежным классам). Теорема Лагранжа, ее следствия и невозможность обращения. Задание группы порождающими соотношениями.	6	3, 4	2	4	4	
3.	**Лекция 3.** Нормальные делители (нормальные подгруппы). Фактор-группы. Критерий нормальности делителя через сопряженные элементы.	6	5, 6	2	4	5	
4.	**Лекция 4.** Гомоморфизм. Ядро и образ гомоморфизма. Естественный (канонический) гомоморфизм. Свойства гомоморфизмов групп. Теорема о гомоморфизмах групп.	6	7, 8	2	4	4	
5.	**Лекция 5. Кольца.** Кольцо (определение, простейшие свойства, терминология). Кольцо классов вычетов. Свойства сравнений. Корректность операций в кольце классов вычетов. Гомоморфизмы и изоморфизмы колец. Теорема о гомоморфизмах колец.	6	9, 10	2	4	5	Аттестационная контрольная работа №1
6.	**Лекция 6.** Евклидовы кольца. Идеалы. Кольца главных идеалов.	6	11, 12	4	4	4	
7.	**Лекция 7.** Максимальные идеалы. Необходимое и достаточное условие	6	13, 14	2	4	5	

	для кольца классов вычетов быть полем. Кольцо многочленов над полем. Нули многочленов, теорема об остатке и теорема Безу. Неприводимые (простые) многочлены.						
8.	**Лекция 8. Векторные пространства.** Векторное пространство (напоминание определений и свойств, изученных в курсе линейной алгебры). Линейная зависимость. Базис. Лемма Штайнера.	6	15, 16	2	4	4	
9.	**Лекция 9.** Изоморфизм векторных пространств. Линейные функционалы. Сопряжённое пространство.	6	17	1	2	3	
10.	**Лекция 10.** Тело, поле (определение, терминология, примеры).	6					Аттестационная контрольная работа №2
11.	**Лекция 11. Поля.** Конечные поля. Число элементов в конечном поле характеристики p. Существование полей порядка pm для всех простых p и натуральных m.	6					
12.	**Лекция 12.** Существование в конечном поле примитивного элемента (с доказательством вспомогательной леммы из теории групп). Уравнение, которому удовлетворяют все элементы конечного поля. Мультипликативная группа поля.	6					
13.	**Лекция 13.** Минимальный многочлен (минимальная функция элемента поля). Минимальный многочлен элемента {x} в F[x]/(g(x)).	6					
14.	**Лекция 14.** Теорема о разложении многочлена Xq^m-X на множители (с доказательством всех вспомогательных лемм). Корни многочленов над конечном полем.	6					
15.	**Лекция 15. Кодирование** Кодирование. Основная задача теории кодирования. Коды Боуза-Чоудхури-Хоквингема (БЧХ). Оценка расстояния между кодовыми вершинами БЧХ. Теорема о линейной независимости в проверочной матрице.	6					Аттестационная контрольная работа №3

16.	**Лекция 16.** Структура идеалов в F[x]/(g(x)). Циклические линейные подпространства классов вычетов. Другие подходы к кодированию. Матрица Адамара. Примеры кодов.	6					
17.	**Лекция 17. Булевы алгебры** Аксиоматика булевой алгебры. Алгебры множеств. Изоморфизмы булевых алгебр. Теорема Стоуна.	6					
	Итого за VI семестр			**34**	**34**	**40**	Зачет
18.	**Лекция 1. Отношения и соответствия** Декартово произведение множеств и отношения. Однородные отношения. Отношение эквивалентности. Пространства толерантности. Соответствия. Основные свойства отображений.	7	18, 19	2	4	5	
19.	**Лекция 2. Частично упорядоченные множества** Предпорядки и порядки. Особые элементы и основные свойства частично упорядоченных (ч. у.) множеств. Грани, изотонные отображения и порядковые идеалы. Операции над ч. у. множествами. Линеаризация. Размерность ч. у. множеств. Вполне упорядоченные множества и смежные вопросы. Некоторые применения теории ч. у. множеств	7	20, 21	4	4	4	
20.	**Лекция 3. Решётки** Определение и основные свойства. Гомоморфизмы, идеалы, фильтры. Модулярные и дистрибутивные решётки. Решётки с дополнениями. Применение теории решёток к задаче классификации.	7	22, 23	4	4	5	Аттестационная контрольная работа №4
21.	**Лекция 4. Булевы алгебры (продолжение)** Булевы алгебры как решётки. Идеалы, фильтры и конгруэнции. Булевы многочлены. Булевы уравнения.	7	24, 25	2	4	4	
22.	**Лекция 5. Идемпотентная алгебра** Тропическая математика. Полуполе обобщенных сумм. Уравнения, операция вычитания и отношение по-	7	26, 27	2	4	5	Аттестационная контрольная работа №5

	рядка. Действия над векторами. Действия над матрицами.						
23.	**Лекция 6. Алгебраические основы криптографии** Основные понятия. Система шифрования RSA. Факторизация натуральных чисел. Дискретное логарифмирование. Криптосистемы МакЭлиса и Нидеррайтера.	7	28, 29	2	4	4	
24.	**Лекция 7. Комбинаторика конечных множеств.** Классические перечислительные и экстремальные проблемы на семействе подмножеств конечного множества. Оценка мощности семейства подмножеств с определёнными ограничениями на пересечения. Стандартные теоретико-числовые задачи, связанные с классическими функциями теории чисел: $\tau(n)$, $\sigma(n)$, $\varphi(n)$, $\pi(n)$. Комбинаторные задачи, связанные с представлениями булевых функций.	7	30, 31	2	4	5	
25.	**Лекция 8. Метод производящих функций.** Классические линейные диофантовы уравнения, выражение числа решений таких уравнений через контурные интегралы. Теория действий групп преобразований на конечном множестве. Лемма Бернсайда и производящие функции для числа разбиений чисел, множеств и перестановок.	7	32, 33		4	4	Аттестационная контрольная работа №6
26.	**Лекция 9. Верхние и нижние оценки.** Методы получения нижних и верхних границ разного типа в задачах, связанных с теорией информации. Методы криптографической защиты сообщений с помощью теоретико-числовых соображений, связанных с группой Эйлера.	7	34	1	2	3	
	Итого за VII семестр			**17**	**34**	**57**	Экзамен (1ЗЕТ – 36 часов)
	Итого			**34**	**68**	**78**	

4.2. Содержание практических занятий

№ п/п	**№ лк из рабочей программы**	**Наименование тем практического занятия**	**Кол-во часов**	**Рекомендуемая литература. №**

				источника
1.	1	Группы. Введение. Алгебра. Алгебраические операции. Группа (определение, простейшие свойства, примеры, терминология). Все конечные группы малых порядков. Симметрические группы. Циклические группы. Подгруппы. Все конечные группы малых порядков. Симметрические группы. Циклические группы. Подгруппы.	2	1,2
2.	2	Группа автоморфизмов. Перестановки. Теорема Кэли. Смежные классы. Отношение эквивалентности в группе (через принадлежность смежным классам). Теорема Лагранжа, ее следствия и невозможность обращения. Задание группы порождающими соотношениями.	2	1,3
3.	3	Нормальные делители (нормальные подгруппы). Факторгруппы. Критерий нормальности делителя через сопряженные элементы.	2	2
4.	4	Гомоморфизм. Ядро и образ гомоморфизма. Естественный (канонический) гомоморфизм. Свойства гомоморфизмов групп. Теорема о гомоморфизмах групп.	2	2,4
5.	5	Кольца. Кольцо (определение, простейшие свойства, терминология). Кольцо классов вычетов. Свойства сравнений. Корректность операций в кольце классов вычетов. Гомоморфизмы и изоморфизмы колец. Теорема о гомоморфизмах колец.	2	2
6.	6	Евклидовы кольца. Идеалы. Кольца главных идеалов.	2	3,4
7.	7	Максимальные идеалы. Необходимое и достаточное условие для кольца классов вычетов быть полем. Кольцо многочленов над полем. Нули многочленов, теорема об остатке и теорема Безу. Неприводимые (простые) многочлены.	2	1,2
8.	8	Векторные пространства. Векторное пространство (напоминание определений и свойств, изученных в курсе линейной алгебры). Линейная зависимость. Базис. Лемма Штайнера.	2	1,3
9.	9	Изоморфизм векторных пространств. Линейные функционалы. Сопряжённое пространство.	2	2
10.	10	Тело, поле (определение, терминология, примеры).	2	2,4
11.	11	Поля. Конечные поля. Число элементов в конечном поле характеристики p. Существование полей порядка pm для всех простых p и натуральных m.	2	2
12.	12	Существование в конечном поле примитивного элемента (с доказательством вспомогательной леммы из теории групп). Уравнение, которому удовлетворяют все элементы конечного поля. Мультипликативная группа поля.	2	3,4
13.	13	Минимальный многочлен (минимальная функция элемента поля). Минимальный многочлен элемента {x} в F[x]/(g(x)).	2	1,2
14.	14	Теорема о разложении многочлена Xq^m-X на множители (с доказательством всех вспомогательных лемм). Корни многочленов над конечном полем.	2	1,3

15.	15	Кодирование. Основная задача теории кодирования. Коды Боуза-Чоудхури-Хоквингема (БЧХ). Оценка расстояния между кодовыми вершинами БЧХ. Теорема о линейной независимости в проверочной матрице.	2	2
16.	16	Структура идеалов в F[x]/(g(x)). Циклические линейные подпространства классов вычетов. Другие подходы к кодированию. Матрица Адамара. Примеры кодов.	2	2,4
17.	17	Булевы алгебры. Аксиоматика булевой алгебры. Алгебры множеств. Изоморфизмы булевых алгебр. Теорема Стоуна.	2	2
		Итого за VI семестр	34	
18.	18	Отношения и соответствия. Декартово произведение множеств и отношения. Однородные отношения. Отношение эквивалентности. Пространства толерантности. Соответствия. Основные свойства отображений.	4	3,4
19.	19	Частично упорядоченные множества. Предпорядки и порядки. Особые элементы и основные свойства частично упорядоченных (ч. у.) множеств. Грани, изотонные отображения и порядковые идеалы. Операции над ч. у. множествами. Линеаризация. Размерность ч. у. множеств. Вполне упорядоченные множества и смежные вопросы. Некоторые применения теории ч. у. множеств	4	
20.	20	Решётки Определение и основные свойства. Гомоморфизмы, идеалы, фильтры. Модулярные и дистрибутивные решётки. Решётки с дополнениями. Применение теории решёток к задаче классификации.	4	
21.	21	Булевы алгебры (продолжение) Булевы алгебры как решётки. Идеалы, фильтры и конгруэнции. Булевы многочлены. Булевы уравнения.	4	
22.	22	Идемпотентная алгебра Тропическая математика. Полуполе обобщенных сумм. Уравнения, операция вычитания и отношение порядка. Действия над векторами. Действия над матрицами.	4	
23.	23	Алгебраические основы криптографии Основные понятия. Система шифрования RSA. Факторизация натуральных чисел. Дискретное логарифмирование. Криптосистемы МакЭлиса и Нидеррайтера.	4	
24.	24	Комбинаторика конечных множеств. Классические перечислительные и экстремальные проблемы на семействе подмножеств конечного множества. Оценка мощности семейства подмножеств с определёнными ограничениями на пересечения. Стандартные теоретико-числовые задачи, связанные с классическими функциями теории чисел: $\tau(n)$, $\sigma(n)$, $\varphi(n)$, $\pi(n)$. Комбинаторные задачи, связанные с представлениями булевых функций.	4	

25.	25	Метод производящих функций. Классические линейные диофантовы уравнения, выражение числа решений таких уравнений через контурные интегралы. Теория действий групп преобразований на конечном множестве. Лемма Бернсайда и производящие функции для числа разбиений чисел, множеств и перестановок.	4	
26.	26	Верхние и нижние оценки. Методы получения нижних и верхних границ разного типа в задачах, связанных с теорией информации. Методы криптографической защиты сообщений с помощью теоретико-числовых соображений, связанных с группой Эйлера.	2	
		Итого за VII семестр	**34**	
		Итого	**68**	

4.3. Тематика для самостоятельной работы студента

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов из содержания дисциплины	Рекомендуемая литература и источники информации	Форма контроля СРС
1	**2**	**3**	**4**	**5**
1.	Общие сведения о дифференциальных уравнениях. Основные понятия. Задачи, приводящие к дифференциальным уравнениям. Дифференциальные уравнения первого порядка. Основные понятия.	5	1,2	ПЗ
2.	Уравнения с разделяющимися переменными. Однородные дифференциальные уравнения.	4	1, 2	ПЗ
3.	Линейные уравнения. Уравнение Я. Бернулли.	5	1, 2	ПЗ, КР
4.	Уравнение в полных дифференциалах. Интегрирующий множитель. Уравнения Лагранжа и Клеро.	4	1, 2	ПЗ
5.	Дифференциальные уравнения высших порядков Основные понятия. Уравнения, допускающие понижение порядка.	5	1, 4	ПЗ, КР
6.	Линейные дифференциальные уравнения высших порядков. Линейные однородные ДУ второго порядка. Линейные однородные ДУ n-го порядка.	4	1, 3	ПЗ
7.	Интегрирование ДУ второго порядка с постоянными коэффициентами. Интегрирование ЛОДУ второго порядка с постоянными коэффициента-	5	2, 3	ПЗ, КР

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов из содержания дисциплины	Рекомендуемая литература и источники информации	Форма контроля СРС
1	2	3	4	5
	ми.			
8.	Интегрирование ЛОДУ n-го порядка с постоянными коэффициентами. Линейные неоднородные дифференциальные уравнения (ЛНДУ).	4	3	ПЗ
9.	Структура общего решения ЛНДУ второго порядка.	3	2	ПЗ
10.	Метод вариации произвольных постоянных. Интегрирование ЛНДУ второго порядка с постоянными коэффициентами и правой частью специального вида Интегрирование ЛНДУ n-го порядка (n > 2) с постоянными коэффициентами и правой частью специального вида.	5	1, 4	ПЗ
11.	Задачи, приводящие к понятию систем дифференциальных уравнений. Нормальные системы дифференциальных уравнений. Метод исключения. Метод интегрируемых комбинаций.	4	1, 2	ПЗ, КР
12.	Системы линейных диффеернциальных уравнений. Интегрирование однородных систем дифференциальных уравнений. Интегрирование однородных систем дифференциальных уравнений.	5	2, 4	ПЗ
13.	Линейные неоднородные системы дифференциальных уравнений	4	3, 4	ПЗ
14.	Системы линейных дифференциальных уравнений с постоянными коэффициентами. Собственные значения и собственные векторы. Линейные однородные системы дифференциальных уравнений с постоянными коэффициентами. Метод Эйлера	5	1, 3	ПЗ
15.	Дифференциальные уравнения с частными производными. Уравнения первого порядка. Линейные однородные уравнения. Задача Коши для линейного однородного уравнения. Квазилинейные уравнения.	4	1, 4	ПЗ, КР
16.	Классификация уравнений второго порядка. Основные определения. Приведение к каноническому виду линейных относительно старших производных уравнений второго порядка с двумя независимыми переменными. Задачи с начальными данными.	5	1, 2	ПЗ
17.	Основные уравнения математической физики Уравнение колебаний струны. Уравнение теплопроводности. Основные уравнения математической физики. Уравнение Лапласа.	4	2	ПЗ

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов из содержания дисциплины	Рекомендуемая литература и источники информации	Форма контроля СРС
1	**2**	**3**	**4**	**5**
18.	Понятие о теории устойчивости Ляпунова. Поведение траектории дифференциального уравнения в окрестности особой точки	3	2,4	ПЗ
	Итого:	**78**		

5. Образовательные технологии.

В процессе занятий используются следующие образовательные, и научно-исследовательские технологии: проблемная лекция и лекция-визуализация, работа в интернет-классе. На семинарах, в свою очередь, студенты выступают с сообщениями, рефератами, проводятся дискуссии, эвристические беседы, деловые игры, используется метод «мозгового штурма». Проверка знаний проводится как в форме письменных контрольных работ и устного опроса, так и в форме блиц-опроса, тестирования, коллоквиума.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий, т.е. 13 часов.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины (модуля).

Входная контрольная работа:

1. Матрицы, определители.
2. Производная.
3. Неопределенные интегралы и их свойства.
4. Методы интегрирования

Вопросы к зачету:

1. Алгебра. Алгебраические операции.
2. Группа (определение, простейшие свойства, примеры, терминология).
3. Симметрические группы. Циклические группы.
4. Подгруппы.
5. Симметрические группы. Циклические группы. Подгруппы.
6. Теорема Кэли.
7. Смежные классы. Отношение эквивалентности в группе
8. Теорема Лагранжа, ее следствия и невозможность обращения.
9. Критерий нормальности делителя через сопряженные элементы.
10. Гомоморфизм. Ядро и образ гомоморфизма.
11. Кольцо (определение, простейшие свойства, терминология).
12. Кольцо классов вычетов.

13. Евклидовы кольца.
14. Идеалы. Кольца главных идеалов.
15. Кольцо многочленов над полем.
16. Векторное пространство.
17. Линейная зависимость. Базис. Лемма Штайнера.
18. Поля. Конечные поля.
19. Мультипликативная группа поля.
20. Основная задача теории кодирования.
21. Коды Боуза-Чоудхури-Хоквингема
22. Булевы алгебры. Аксиоматика булевой алгебры. Алгебры множеств. Изоморфизмы булевых алгебр. Теорема Стоуна.

Вопросы к экзамену:

1. Отношения и соответствия. Декартово произведение множеств и отношения. Однородные отношения. Отношение эквивалентности.
2. Пространства толерантности. Соответствия. Основные свойства отображений.
3. Частично упорядоченные множества.
4. Особые элементы и основные свойства частично упорядоченных множеств.
5. Решетки. Определение и основные свойства.
6. Гомоморфизмы, идеалы, фильтры. Модулярные и дистрибутивные решётки.
7. Решётки с дополнениями.
8. Булевы алгебры как решётки. Идеалы, фильтры и конгруэнции.
9. Булевы многочлены. Булевы уравнения.
10. Идемпотентная алгебра
11. Полуполе обобщенных сумм.
12. Алгебраические основы криптографии
13. Система шифрования RSA. Факторизация натуральных чисел.
14. Дискретное логарифмирование.
15. Криптосистемы МакЭлиса и Нидеррайтера.
16. Комбинаторика конечных множеств.
17. Комбинаторные задачи, связанные с представлениями булевых функций.
18. Метод производящих функций.
19. Классические линейные диофантовы уравнения, выражение числа решений таких уравнений через контурные интегралы.
20. Теория действий групп преобразований на конечном множестве.
21. Методы криптографической защиты сообщений с помощью теоретико-числовых соображений, связанных с группой Эйлера.

Вопросы для проверки остаточных знаний

1. Алгебра.
2. Группа
3. Циклические группы.
4. Подгруппы.
5. Гомоморфизм. Ядро и образ гомоморфизма.
6. Кольцо Кольцо классов вычетов.
7. Евклидовы кольца.

8. Идеалы. Кольца главных идеалов.
9. Поля. Конечные поля.
10. Булевы алгебры. Аксиоматика булевой алгебры.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Для самостоятельной работы студентов по дисциплине – Б1.В.ОД.8 – «Прикладная алгебра» сформированы следующие виды учебно-методических материалов:

1. Фонд оценочных средств.
2. Основная и дополнительная литература.
3. Методические указания по выполнению практических заданий в электронном формате.
4. Список адресов сайтов сети Интернет, содержащих актуальную информацию по изучаемой дисциплине.
5. Список Интернет-ресурсов, содержащих актуальную информацию по изучаемой дисциплине.

Самостоятельная работа студентов описывается и регулируется:

- Методическими рекомендациями по дисциплине;
- Методическими рекомендациями по организации самостоятельной работы студентов ДГТУ;
- Положением об организации самостоятельной (внеаудиторной) работы студентов, обучающихся по программам высшего образования в ДГТУ.

Самостоятельная работа по данной дисциплине включает в себя:

- подготовку к текущим лекционным занятиям с использованием интерактивных обучающих средств;
- подготовку и выполнение лабораторных работ, в том числе с использованием программ компьютерного моделирования;
- подготовку и выполнение практических работ;
- выполнение заданий в электронном виде;
- подготовку к текущим контрольным мероприятиям, включая опросы, собеседования, контрольные работы, рефераты;
- выполнение индивидуальных заданий (реферат, вопросы дискуссий);
- подготовку к текущей и промежуточной (семестровой) аттестации в форме тестирования.

7.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Основная литература:

1. Биркгоф Г., Барти Т. Современная прикладная алгебра. М.: Мир. 1976.
2. Гуров С.И. Упорядоченные множества и универсальная алгебра (вводный курс). М.: ВМК МГУ. 2004.
3. Гуров С.И. Лекции по упорядоченным множествам и универсальной алгебре. М.: ВМК МГУ (в печати).
4. Курош А.Г. Общая алгебра (лекции 1969 1970 учебного года). М.: Наука. 1974.
5. Мальцев А.И. Алгебраические системы. М.: Наука. 1970.
6. Скорняков Л.А. Элементы общей алгебры. М.: Наука. 1983.

Дополнительная литература:

1. Владимиров Д.А. Булевы алгебры. М.: Наука. 1969.

2. Кон П. Универсальная алгебра. М.: Мир. 1968.

3. Лидл Р., Пильц Г. Прикладная абстрактная алгебра. Екатеринбург: Изд-во Урал. ун-та. 1996.

4. Плоткин Б.И. Универсальная алгебра, алгебраическая логика и базы данных. М.: Наука. 1991.

7.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:
– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:
– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:
– в форме электронного документа;
– в печатной форме.

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Электронно-библиотечная система IPRbooks [Электронный ресурс]. - Режим доступа: http://www.iprbookshop.ru/

2. Издательство «Лань» [Электронный ресурс]: электронно-библиотечная система. – URL:http://elanboobok.com/

3. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс]. – URL:http://scool-collection.edu.ru/

4. Единое окно доступа к образовательным ресурсам [Электронный ресурс]. – URL:http://window.edu.ru/

5. Антиплагиат [Электронный ресурс]. – Режим доступа - URL:http:// www.antiplagiat.ru/index.aspx

6. Информационная система доступа к электронным каталогам библиотек сферы образования и науки (ИС ЭКБСОН) [Электронный ресурс] Режим доступа: http://www.vlibrary.ru/

7.4. Методические указания для обучающихся при освоении дисциплины

В процессе освоения дисциплины Б1.В.ОД.8 – «Прикладная алгебра» предусматривается использование следующих образовательных технологий для формирования компетенций:

- при проведении лекционных занятий (передача учебной информации от преподавателя к студентам) - интерактивные формы проведения занятий; применение компьютерных (мультимедийных) технологий и технических средств. Студенты являются активными участниками занятия, отвечающими на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию у студентов процессов усвоения материала. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установ-

ления связей с ранее освоенным материалом. На лекциях комбинируются экстраактивная форма проведения, т.е. репродукция знаний только преподавателем в меньшем объеме аудиторных занятий (30-40%) и интерактивная форма проведения, т.е. режим диалоговых технологий студента и преподавателя, в большем объеме аудиторных занятий (60-70%). Эффективной интерактивной формой лекции предлагается проблемный метод ее проведения;

- при проведении практических занятий (решение конкретных практических примеров и задач на основании теоретических знаний) - активные и интерактивные формы проведения занятий; применение компьютерных технологий;

При подготовке к практическим занятиям используется опережающая самостоятельная работа, т.е. изучение студентами нового материала до его изучения в ходе аудиторных занятий (лекции).

Работа на практических занятиях предполагает активное участие в дискуссиях. Для подготовки к занятиям рекомендуется выделять в материале проблемные вопросы, затрагиваемые преподавателем в лекции, и группировать информацию вокруг них. Желательно выделять в используемой литературе постановки вопросов, на которые разными авторам могут быть даны различные ответы. На основании постановки таких вопросов следует собирать аргументы в пользу различных вариантов решения поставленных проблем.

Практические занятия имеют важнейшее значение для усвоения программного материала.

Задачи практических занятий:

- закрепление знаний путем решения ситуационных задач;
- развитие способности самостоятельно использовать полученные знания;
- приобретение навыков самостоятельного анализа проблемной ситуации;
- приведение разрозненных знаний в определенную систему;
-ознакомление с методами и средствами анализа данных в их практическом применении;

Для эффективного изучения теоретической части дисциплины необходимо:

- построить работу по освоению дисциплины в порядке, отвечающим изучению основных этапов, согласно приведенным темам лекционного материала;
- систематически проверять свои знания по контрольным вопросам;
- усвоить содержание ключевых понятий;
- активно работать с основной и дополнительной литературой по соответствующим темам.

Для эффективного изучения практической части дисциплины настоятельно рекомендуется:

- систематически выполнять подготовку к лекционным занятиям по предложенным преподавателем темам.

Следует стараться избегать необоснованных пропусков аудиторных занятий. Необходимо учиться преодолевать самый высокий уровень непонимания материала («всё непонятно»).

При разборе примеров в аудитории или при выполнении домашних заданий целесообразно каждый шаг обосновывать теми или иными теоретическими положениями.

При изучении теоретического материала не задерживать внимание на трудных и непонятных местах, смело их пропускать и двигаться дальше, а затем возвращаться к тому, что было пропущено (часто последующее проясняет предыдущее).

Начальное ознакомление с проблемой осуществить по литературным источникам. Промежуточный контроль позволяет оценить знания студента по балльно-рейтинговой системе.

Дополнительно баллы можно получить за творческие успехи и индивидуальный подход при выполнении лабораторных работ. Баллы могут быть сняты за пропуски занятий без уважительной причины.

В фонде оценочных средств дисциплины приведены образцы контролирующих материалов для оценки знаний студентов, которые содержат вопросы теоретического и практического характера. Вопросы теоретического характера могут быть либо в форме тестов, либо в форме письменных заданий.

При работе с терминами необходимо обращаться к словарям, в том числе доступным в Интернете, например на сайте http://dic.academic.ru.

Перечень заданий для самостоятельной работы разрабатываются преподавателем, ведущим дисциплину, с учётом особенностей образования и интересов обучающихся. При написании рефератов в материале следует выделить небольшое количество (не более 5) заинтересовавших Вас проблем и сгруппировать материал вокруг них. Следует добиваться чёткого разграничения отдельных проблем и выделения их частных моментов.

Дополнительно темы рефератов и творческих заданий могут быть предложены обучающимися самостоятельно и согласованные с преподавателем.

В рамках изучаемой дисциплины используются темы рефератов, предполагающие более углублённое изучение вопросов, рассмотренных на лекциях, или изучение дополнительных вопросов, не рассматриваемых на лекциях, но имеющих непосредственное отношение к изучаемым темам. Темы творческих заданий предполагают выполнение обучающимся работы, направленной на закрепление практических навыков, в целях их последующего применения в профессиональной деятельности.

Написание реферата и выполнение творческого задания включает в себя следующие виды самостоятельной работы:

- работа с различными источниками информации: изучение основной и дополнительной литературы, использование справочно-правовых систем, компьютерной техники и Интернета;
- оформление реферата (творческого задания);
- сообщение по теме реферата (творческого задания) в форме доклада на 10 минут с презентацией.

При подготовке к выполнению реферата необходимо изучить основную и дополнительную литературу, нормативные правовые документы и Интернет-ресурсы, указанные в программе курса.

Перед выполнением реферата (творческого задания) обучающийся должен внимательно выслушать инструктаж преподавателя по выполнению задания, а также обсудить цель, содержание, сроки выполнения, ориентировочный объем работы, необходимый перечень литературы и нормативных источников, основные требования к результатам работы, критерии оценки реферата. Преподаватель предупреждает обучающийся о возможных типичных ошибках, встречающихся при выполнении задания.

При подготовке к экзамену необходимо опираться, прежде всего, на лекции, а также на источники, которые разбирались на семинарах в течение семестра.

При организации самостоятельной работы студентов (изучение студентами теоретического материала, подготовка к лекциям, практическим занятиям) используются следующие образовательные технологии:

- технология разноуровневого (дифференцированного) обучения;
- технология модульного обучения;
- технология использования компьютерных программ;
- Интернет-технологии;
- технология тестирования.

На самостоятельной работе студентами применяется деятельностный подход и учебно – исследовательский метод обучения, т.е. студенты самостоятельно изучают объекты, процессы и явления, уже известные в области моделирования биологических процессов и систем, но неизвестные им, применяя при этом методы научно – технического познания, изложенные выше.

Применение вышеназванных методов обучения позволяют студентам усвоить содержание дисциплины и ускорить формирование у них таких общеучебных умений и навыков как логическое мышление, алгоритмизация, моделирование, анализ, синтез, индукция - дедукция, «свертывание» информации до понятий, «развертывание» информации из понятий и т.д.

Реализация компетентностного и личностно-деятельностного подхода с использованием перечисленных технологий предусматривает активные и интерактивные формы обучения. Удельный вес занятий, проводимых в интерактивных формах, составляет не менее 20 % аудиторных занятий.

7.5. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине

При осуществлении образовательного процесса по дисциплине Б1.В.ОД.8 – «Прикладная алгебра» используются следующие информационные технологии:

1. Internet – технологии:

-WWW (англ. World Wide Web – Всемирная Паутина) – технология работы в сети с гипертекстами;

- FTP (англ. File Transfer Protocol – протокол передачи файлов) – технология передачи по сети файлов произвольного формата;

- IRC (англ. Internet Relay Chat – поочередный разговор в сети, чат) – технология ведения переговоров в реальном масштабе времени, дающая возможность разговаривать с другими людьми по сети в режиме прямого диалога;

- ICQ (англ. I seek you – я ищу тебя, можно записать тремя указанными буквами) – технология ведения переговоров один на один в синхронном режиме.

2. Дистанционное обучение с использованием ЭИОС на платформе Moodle.

3. Технология мультимедиа в режиме диалога.

4. Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории).

5. Гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии):

8. Описание материально-технической базы, используемой (необходимой) для осуществления образовательного процесса по дисциплине

Лекционные занятия по дисциплине Б1.В.ОД.8 – «Прикладная алгебра» осуществляются в учебных аудиториях, рассчитанных на 25 студентов, снабженное необходимым количеством посадочных мест (один стол на двух обучающихся, стулья).

Лекционные аудитории оборудованы мультимедийными комплексами и экранами для демонстрации слайдовых презентаций и иных форм визуализации учебного материала дисциплины. Для демонстрации презентаций студентов использоваться мультимедийные средства, имеющиеся в распоряжении кафедры (проектор, экран, ноутбук).

Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB, audio, IDMI.

Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и

доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет.

Повышение эффективности изучения учебной дисциплины по данной программе и её усвоения студентами предполагает возможность визуализации информации, излагаемой преподавателем в рамках лекционных занятий, которая может осуществляться в форме подготовки электронных «презентаций» к отдельным лекциям в рамках учебного курса.

Презентации к определенным лекционным занятиям позволяют проиллюстрировать основные тезисы учебной темы и ключевые мысли преподавателя, которые студентам необходимо зафиксировать в письменном виде. Использование преподавателем презентаций на лекционных занятиях может осуществляться только с использованием компьютера, проекционного оборудования и экрана, необходимых для обеспечения визуализации основных теоретических положений в рамках каждого из занятий.

Для проведения аудиторных занятий и внеаудиторной самостоятельной работы студентов имеются компьютерные классы и Интернет – центр с доступом к сети. Дисциплина обеспечена учебно-лабораторным оборудованием, требуемым для видов учебной работы согласно ФГОС направления подготовки бакалавров.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов с нарушениями слуха предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов с нарушениями зрениями предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов с нарушениями опорно-двигательного аппарата используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ООП ВО для направления 01.03.02 – Прикладная математика и информатика, по профилю – «Системное программирование и компьютерные технологии»

Рецензент от выпускающей кафедры

_____ _____

Подпись ФИО